REMARKS

STATUS OF THE CLAIMS

Claims 1-3, 6, 9-11, and 13-16 are pending in the application.

Claims 3 and 11 are rejected under 35 USC 103(a) as being unpatentable over Bruce Schneier, "Applied Cryptography."

Claims 1, 10, and 14-16 are rejected under 35 USC 103(a) as being unpatentable over Bruce Schneier, "Applied Cryptography" in view of Colvin, Sr. (U.S. Patent No. 6,041,123). Colvin is newly relied upon.

Claims 2, 5, 6 and 9 are rejected under 35 USC 103(a) as being unpatentable over Bruce Schneier, "Applied Cryptography" in view of Barrett et al. (U.S. Patent No. 5,222,137).

Claim 13 is rejected under 35 USC 103(a) as being unpatentable over Bruce Schneier, "Applied Cryptography" in view of '123 in further view of "Mapping a Network Drive."

Claims 1, 3, 6, 9, 10, 11, 13, 14, 15 and 16 are amended, new claim 17 is added, and, thus, claims 1-3, 6, 9-11, and 13-17 remain pending for reconsideration, which is respectfully requested.

No new matter has been added in this Amendment.

REJECTIONS

The Response to Arguments is one page 2, items 4-5, in which the Office Action provides that the previous arguments have not been persuasive, because the Examiner disagrees that both an individual key and a communication key are used at the transmission side. The Examiner asserts that the "transmission side" can be interpreted as any processing during transmission and before receipt at destination.

The Examiner appears to assert that Schneier's FIG. 10.1 shows multiple nodes and if a transmission side is Node 1 and a destination side is Node 4, then essentially the transmission side nodes become Nodes 1-3, which use Ek1, Ek2 and Ek3, etc. for encryption. In other words, the Examiner appears to be relying on the Schneier sentence in page 217, "On the other hand, any intelligent switching or storing nodes between the sender and the receiver need to decrypt the data stream before processing it."

The independent claims are 1, 3, 6, 9, 10, 11, 14, 15 and 16, which are further amended, using claims 1 and 3 as examples, as follows:

1. (CURRENTLY AMENDED) A cryptographic communication method, comprising:

individually authenticating, in ~~a~~each transmission side, a common communication key and an individual transmission side only key that is different from the common communication key, thereby using both keys to encipher or decode in each transmission side,

determining, in ~~the~~each transmission side, whether a target file is enciphered by the individual transmission side only key,

decoding the target file using the individual transmission side only key, if determined that the target file is enciphered, and not decode processing the target file as an unprocessed target file, if determined that the target file is not enciphered; and

enciphering for transmission, in ~~the~~each transmission side, the decoded target file or the unprocessed target file that is not enciphered, using the common communication key,

wherein in ~~the~~each transmission side, the decoding using the individual transmission side only key and the enciphering using the common communication key are performed continuously, if the decoding is performed.

3. (CURRENTLY AMENDED) A cryptographic communication method, comprising:

individually authenticating, in ~~a~~each reception side, a common communication key and an individual reception side only key that is different from the common communication key, thereby using both keys to encipher or decode in each reception side;

decoding, in ~~the~~each reception side, the received file using the common communication key;

determining, in ~~the~~each reception side, whether a target folder for storing the decoded file is for encipher files,

enciphering the decoded file using the individual reception side only key and storing the enciphered decoded file in the target folder, if the target folder is for encipher files, and storing the decoded file in the target folder without any encipher processing, if the target folder is not for encipher files,

wherein in ~~the~~each reception side the decoding process using the common communication key and the enciphering

process using the ~~communication~~individual reception side only key are performed continuously, if the enciphering process is performed.

Support for the claim amendments can be found, for example, in page 9, lines 12-13 (individual communication side key KP for a communication side only) and page 11, lines 17-19 and page 12, lines 9-19 of the present Application.

The claims are clarified to emphasize that in contrast to Schneier's link-by-link encryption as illustrated in FIG. 10.1, the claimed present invention provides, "individually authenticating, ***in a~~each~~ transmission side, a common communication key and an individual transmission side only key that is different from the common communication key***, thereby using ***both keys to encipher or decode in each transmission side***" (e.g., claim 1). In particular, the claim amendments clarify that in contrast to, for example, Schneier's Node 2, which uses Dk1 to decrypt and Ek2 to encrypt, the claimed present invention uses "a ***common communication key*** and ***an individual transmission side only key***." In Schneier, DK1 must be in common with Ek1 of Node 1 for decryption in Node 2, and Ek2 must be in common with Dk2 of Node 3 for decryption in Node 3, whereas the claimed present invention in the context of transmission processing provides, "***an individual transmission side only key***" in "***each transmission side.***"

The Office Action rejects independent claims 1, 10, and 14-16 by relying on Colvin. Colvin discloses a Master Key Router that is also connected to a network and the Master Key Router receives encrypted communications from a sending client, decrypts the information, reencrypts the information in a specific manner such that a particular receiving client can decrypt it, and sends the reencrypted information to the receiving client (column 3, lines 6-18). However, Colvin's Master Key Router differs from the claimed present invention's, "individually authenticating, ***in a~~each~~ transmission side, a common communication key and an individual transmission side only key that is different from the common communication key***, thereby using ***both keys to encipher or decode in each transmission side***" (e.g., amended independent claim 1).

The Office Action also rejects independent claims 6 and 9 by relying on Barrett. Barrett discloses "A radio (100) transmits and receives encrypted signals having unencrypted key identifiers, allowing other radios having the corresponding key identifiers and encryption keys to communicate with the radio (100)" (Abstract, column lines 58-63). However, a combination of

Schneier and Barrett fail to disclose or suggest the claimed present invention's:

> 6. (CURRENT AMENDED) A cryptographic communication method, comprising:
>
> authenticating, in a transmission side, an individual transmission side only key,
>
> authenticating a common communication key that is different from the individual side only key from among a plurality of common communication keys,
>
> enciphering data to be transmitted in the transmission side using a common communication key from among ~~a~~the plurality of common communication keys,
>
> determining, in the transmission side, whether a target file is enciphered by the individual transmission side only key,
>
> decoding the target file using the individual transmission side only key, if determined that the target file is enciphered, and not decode processing the target file as an unprocessed target file, if determined that the target file is not enciphered,
>
> enciphering for transmission, in the transmission side, the decoded target file or the unprocessed target file that is not enciphered, using the common communication key,
>
> adding an identification code corresponding to the common communication key used for the enciphering, and
>
> decoding, in the reception side, the enciphered target file received, from the transmission side, using a common communication key, from among a plurality of common communication keys, corresponding to the identification code added in the enciphered target file.

Further, in contrast to the relied upon references, the claimed present invention, using claim 16 as an example, provides:

> 16. (CURRENTLY AMENDED) A cryptographic communication method, comprising:
>
> using a common communication key to a transmission and reception side for enciphering and deciphering data to be transmitted and received by ~~a~~the transmission and reception side, respectively, and
>
> using an individual transmission side only key for decoding enciphered data stored in an enciphered folder at ~~the~~each transmission side and an individual reception side only key for enciphering data to be stored in an enciphered folder at each reception side,

wherein in ~~the~~each transmission side, ~~the individual key is different from the communication key used for enciphering the data to be transmitted~~, first, the stored enciphered data are decoded using the individual transmission side only key ~~first~~, and, second, the decoded data is enciphered using the common communication key for transmission, and

wherein in each reception side, first, the received enciphered data are decoded using the common communication key, and, second, the decoded data is enciphered to be stored in the enciphered folder in the reception side using the individual reception side only key.

In other words, in contrast to the relied upon references of Schneier, Colvin, Barrett and "Mapping a Network Drive," the claimed present invention provides, a "transmission side ***only*** key" and a "reception side ***only*** key" (or a transmission/reception side only key) (emphasis added).

NEW INDEPENDENT CLAIM 17

New independent claim 17 is based upon, for example, independent claim 16 and incorporates additional features of, "preparing ***a transmission and reception folder for storing the file to be transmitted*** by cryptographic communication," and "preparing ***an enciphered folder*** for ***automatically performing an enciphering*** process on a file ***using an individual transmission/reception side only key*** to store the file as an enciphered file ***when the file is moved from another folder to the enciphered folder***, and for ***automatically performing a decoding process*** on the enciphered file stored in the enciphered folder ***using the individual transmission/reception side only key when the enciphered file stored in the enciphered folder is moved to another folder***."

Therefore, in contrast to the relied upon references of Schneier, Colvin, Barrett and "Mapping a Network Drive," the claimed present invention as recited in new independent claim 17 provides:

17. (NEW) A cryptographic communication method, comprising:

using a common communication key for enciphering a file to be transmitted;

preparing ***a transmission and reception folder for storing the file to be transmitted*** by cryptographic communication;

preparing ***an enciphered folder*** for ***automatically performing an enciphering*** process on a file ***using an individual transmission/reception side only key*** to store the file as an enciphered file ***when the file is moved from another folder to the enciphered folder***, and for ***automatically performing a decoding process*** on the enciphered file stored in the enciphered folder ***using the individual transmission/reception side only key when the enciphered file stored in the enciphered folder is moved to another folder***;

decoding the file stored in the enciphered folder ***using the individual transmission/receptions side only key to encipher the decoded file using the common communication key*** for storing the common communication key enciphered file ***in the transmission and reception folder***, when the file stored in the ***enciphered folder is moved to the transmission and reception folder***;

enciphering the file stored in a folder other than the enciphered folder ***using the common communication key*** to store the common communication key enciphered file ***in the transmission and reception folder, when the file stored in the folder other than the enciphered folder is moved to the transmission and reception folder***; and

transmitting the common communication key enciphered file stored in the transmission and reception folder.

Support for the new independent claim 17 (as well as other independent claims) can be found, for example, in FIGS. 7, 14 and 15 and page 16, line 18 to page 21, line 9 of the present Application.

In view of the claim amendments and remarks, withdrawal of the rejection of pending claims and allowance of pending claims is respectfully requested.

CONCLUSION

If there are any formal matters remaining after this response, the Examiner is requested to telephone the undersigned to attend to these matters.

Respectfully submitted,
STAAS & HALSEY LLP

Date: June 16, 2005

By: _____
Mehdi D. Sheikerz
Registration No. 41,307

1201 New York Ave, N.W., Suite 700
Washington, D.C. 20005
Telephone: (202) 434-1500
Facsimile: (202) 434-1501